SPYWOLF

Security Audit Report

Completed on

January 6, 2023

OVERVIEW

This audit has been prepared for **SpaceDoge** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

SpaceDoge

PROJECT DESCRIPTION

According to their whitepaper:

Spacedoge is a Decentralised MemeToken. A revolutionary token inspired by ELON MUSK when he loaded dogecoin into space via Space X rocket and made dogecoin go down in history throughout the crypto world. $SDOGE extends that further by bringing more utilities and ways to earn PASSIVE INCOME.

Release Date: Presale starts in January, 2023

Category: Meme token

CONTRACT INFO

Token Name
SpaceDoge

Symbol
SDOGE

Contract Address
0xfeba2DE3072D57080Fa6A6c73047a9CB65f20548

Network
Binance Smart Chain
~~TETNET~~

Language
Solidity

Deployment Date
Nov 10, 2022

Verified?
Yes

Total Supply
100,000,000,000

Status
Not launched

TAXES

Buy Tax
4%

Sell Tax
4%

*Taxes cannot be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of January 06, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

100,000,000

DEX

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	TESTNET
Uniq Senders	TESTNET
Uniq Receivers	TESTNET
Total Amount	TESTNET
Median Transfer Amount	TESTNET
Average Transfer Amount	TESTNET
First transfer date	TESTNET
Last transfer date	TESTNET
Days token transferred	TESTNET

SMART CONTRACT STATS

Calls Count	TESTNET
External calls	TESTNET
Internal calls	TESTNET
Transactions count	TESTNET
Uniq Callers	TESTNET
Days contract called	TESTNET
Last transaction time	TESTNET
Created	TESTNET
Create TX	TESTNET
Creator	TESTNET

FEATURED WALLETS

Owner address	0xd97d0cb12a9ca7f394c54829ef2dc71361b42a8b
Marketing wallet	0xdD05d097e2E293F53Cd362847fa3B743939F33a6
Salary wallet	0xF8A2645dC25B54CcF5851682B3b3Eb61A902fdB7
LP address	**LP has not yet been added**

PRESALE STATS (Pinksale)

TESTNET CONTRACT

Total Supply	NOT YET LIVE AT THE TIME OF AUDIT
Tokens For Presale	NOT YET LIVE AT THE TIME OF AUDIT
Tokens For Liquidity	NOT YET LIVE AT THE TIME OF AUDIT
Soft Cap	NOT YET LIVE AT THE TIME OF AUDIT
Presale Start Time	NOT YET LIVE AT THE TIME OF AUDIT
Presale End Time	NOT YET LIVE AT THE TIME OF AUDIT
Listing On	NOT YET LIVE AT THE TIME OF AUDIT
Liquidity Percent	NOT YET LIVE AT THE TIME OF AUDIT
Liquidity Lockup Time	NOT YET LIVE AT THE TIME OF AUDIT

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

When takefees _isFeeEnabled variable is true and the contract's balance is above the swap threshold, contract will halt on selling and it will become impossible to sell.

```
function executeSwap(uint256 amount) private {
 ....................
    uint256 bnbToBeAddedToLiquidity = (bnbSwapped *
        tokensToSwapForLiquidity) / 200*2;
    (, uint256 bnbAddedToLiquidity, ) = _pancakeswapV2Router
        .addLiquidityETH{value: bnbToBeAddedToLiquidity}(
        address(this),
        tokensToAddAsLiquidity,
        0,
        0,
        _autoLiquidityWallet,
        block.timestamp + 360
    );
....................
}
```

- Recommendation:
  - There is wrong calculation of bnb/tokens proportion for the tokens reserved for liquidity.
    Auto liquidity add succeeds with the following proportion:
    `uint256 bnbToBeAddedToLiquidity = (bnbSwapped * tokensToSwapForLiquidity) / tokensToSwap;`

FOUND THREATS

⚠ Low Risk

*Owner can set max transaction limit, but cannot lower it than 0.01% of total supply.

```
function setTransactionLimit(uint256 limit) public onlyOwner {
    require(
        limit >= 1 && limit <= 10000,
        "Limit must be greater than 0.01%"
    );
    _transactionLimit = _totalTokens / limit;
}
```

*In order to add liquidity, transaction limit should be equal or above the desired tokens amount for liquidity add.

- Recommendation:
  - Considered as good max transaction limitation practice is max transaction amount to be not lower than 0.1% of total supply.

Informational

Owner can set max claim reward amount allowed.

```
function setMaxClaimAllowed(uint256 value) public onlyOwner {
    require(value > 0, "Value must be greater than zero");
    _maxClaimAllowed = value;
}
```

Owner can change rewards cycle period.

```
function setRewardCyclePeriod(uint256 period) public onlyOwner {
    require(
        period >= 3600 && period <= 86400,
        "RewardCycle must be updated to between 1 and 24 hours"
    );
    _rewardCyclePeriod = period;
}

function setRewardCycleExtensionThreshold(uint256 threshold)
    public
    onlyOwner
{
    _rewardCycleExtensionThreshold = threshold;
}
```

Owner can exclude address from rewards.

```
function setExcludedFromRewards(address addr, bool isExcluded)
    public
    onlyOwner
{
    _addressesExcludedFromRewards[addr] = isExcluded;
    updateAutoClaimQueue(addr);
}
```

Owner can exclude address from fees.

```
function setExcludedFromFees(address addr, bool value) public onlyOwner {
    _addressesExcludedFromFees[addr] = value;
}
```

Informational

Set buy and sell fees functions have onlyOwner modifier but are declared as internal and not accessible after contract deployment.

```
function setBuyFees(
    uint8 liquidityFee,
    uint8 rewardFee,
    uint8 buybackFee,
    uint8 marketingFee,
    uint8 salaryFee
) internal onlyOwner {
    _buyFee.liquidityFee = liquidityFee;
    _buyFee.rewardFee = rewardFee;
    _buyFee.buybackFee = buybackFee;
    _buyFee.marketingFee = marketingFee;
    _buyFee.salaryFee = salaryFee;
}

function setSellFees(
    uint8 liquidityFee,
    uint8 rewardFee,
    uint8 buybackFee,
    uint8 marketingFee,
    uint8 salaryFee
) internal onlyOwner {
    _sellFee.liquidityFee = liquidityFee;
    _sellFee.rewardFee = rewardFee;
    _sellFee.buybackFee = buybackFee;
    _sellFee.marketingFee = marketingFee;
    _sellFee.salaryFee = salaryFee;
}
```

Informational

Owner can change gradual burn periods but cannot lower them below 5 minutes.
Owner can initiate buy and burn with up to 1% of the contract's accumulated bnb balance.
Owner can set buy and burn percent from contract's accumulated bnb balance up to 1% at burn transaction.

```
function setGradualBurnTimespan(uint256 timespan) public onlyOwner {
    require(timespan >= 5 minutes, "Cannot be less than 5 minutes");
    _gradualBurnTimespan = timespan;
}

function buyAndBurn(uint256 bnbAmount) external onlyOwner {
    require(
        bnbAmount <= address(this).balance / 100,
        "Manual burn amount is too high!"
    );
    require(bnbAmount > 0, "Amount must be greater than zero");

    doBuyAndBurn(bnbAmount);
}

function setGradualBurnMagnitude(uint256 magnitude) public onlyOwner {
    require(magnitude <= 100, "Must be equal or less to 100");
    _gradualBurnMagnitude = magnitude;
}

function processGradualBurn() private returns (bool) {
    if (!shouldBurn()) {
        return false;
    }

    uint256 burnAmount = (address(this).balance * _gradualBurnMagnitude) /
        10000;
    doBuyAndBurn(burnAmount);
    return true;
}

function doBuyAndBurn(uint256 bnbAmount) private {
    if (bnbAmount > address(this).balance) {
        bnbAmount = address(this).balance;
    }

    if (bnbAmount == 0) {
        return;
    }

    if (swapBNBForTokens(bnbAmount, BURN_WALLET)) {
        emit Burned(bnbAmount);
    }
```

Recommendations

- Exclude owner/presale address from fees for initial liquidity add or leave _isFeeEnabled to its default value (false).
- For future tax flexibility and full scope contract usage, change visibility of setBuyFees and setSellFees functions from **internal** to **public.** Considered as good practice is buy and sell limits combined not to exceed 25%.
- For initial liquidity add, transaction limit should be equal or above the desired tokens amount for liquidity add.

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Space Doge

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract

There is no information about initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

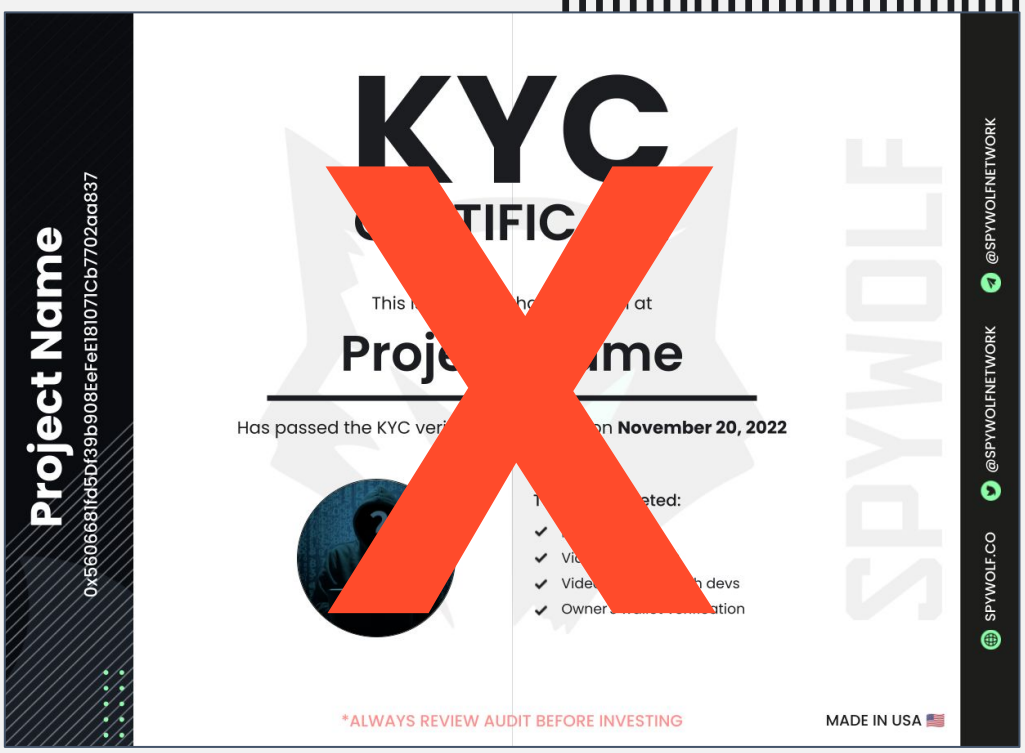
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://spacedoge.club/

Domain Registry
https://www.namecheap.com

Domain Expiration
Expires on 2023-12-27

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

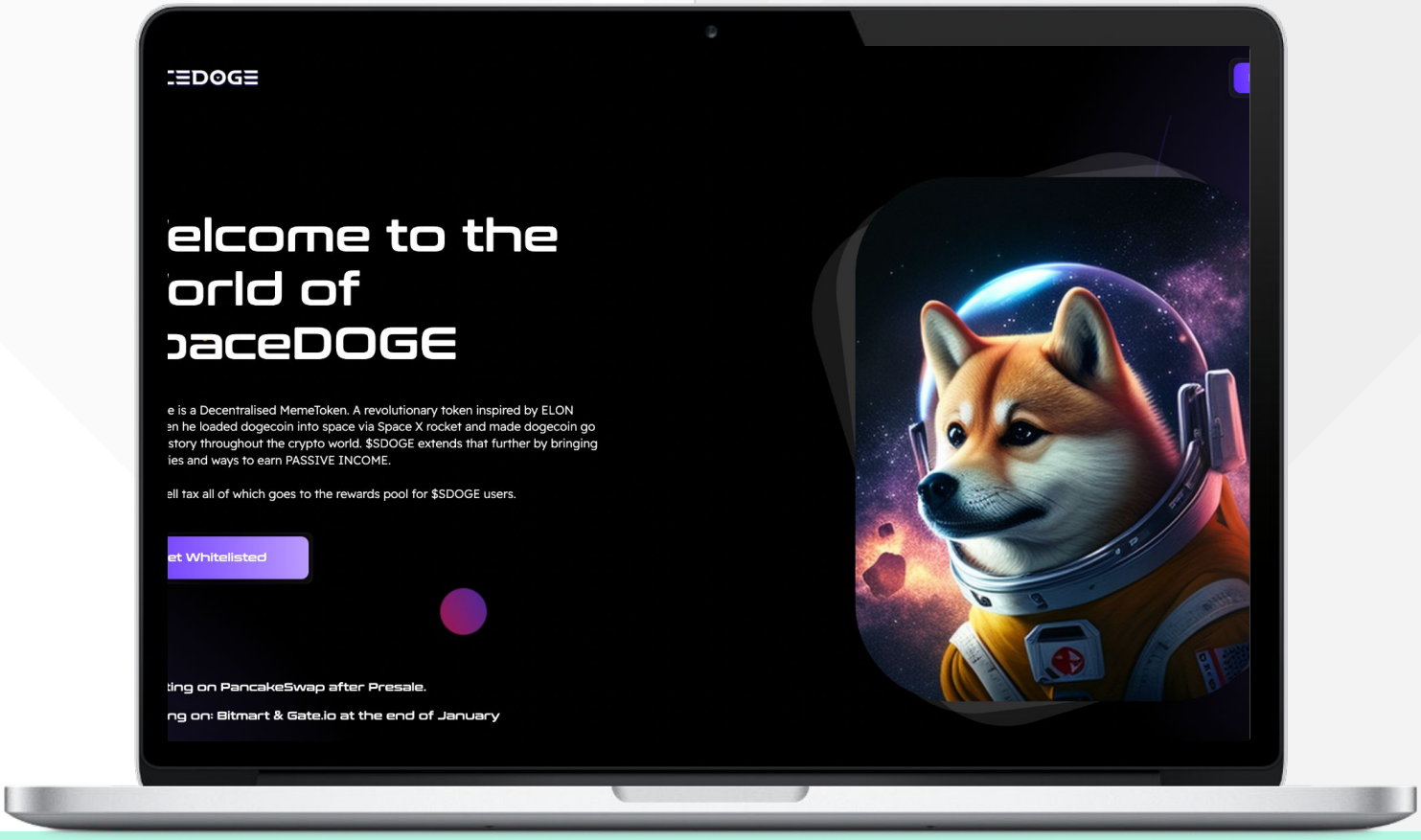
Design
Single page design, appropriate color scheme and very nice graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
No whitepaper.

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes



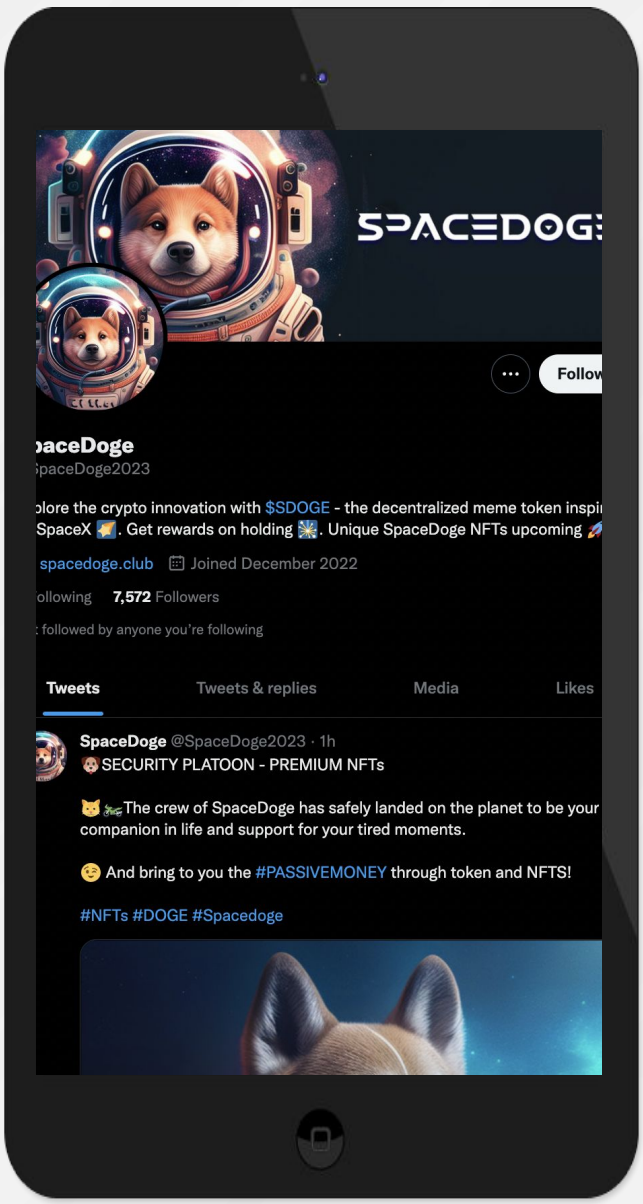
spacedoge.club

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media channels of communication are active



Twitter

@SpaceDoge2023

- 7 558 followers
- Active
- Posts frequently

Discord

- Not available

Telegram

@spacedogeclub

- 22 members
- Channel
- Daily announcements

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.